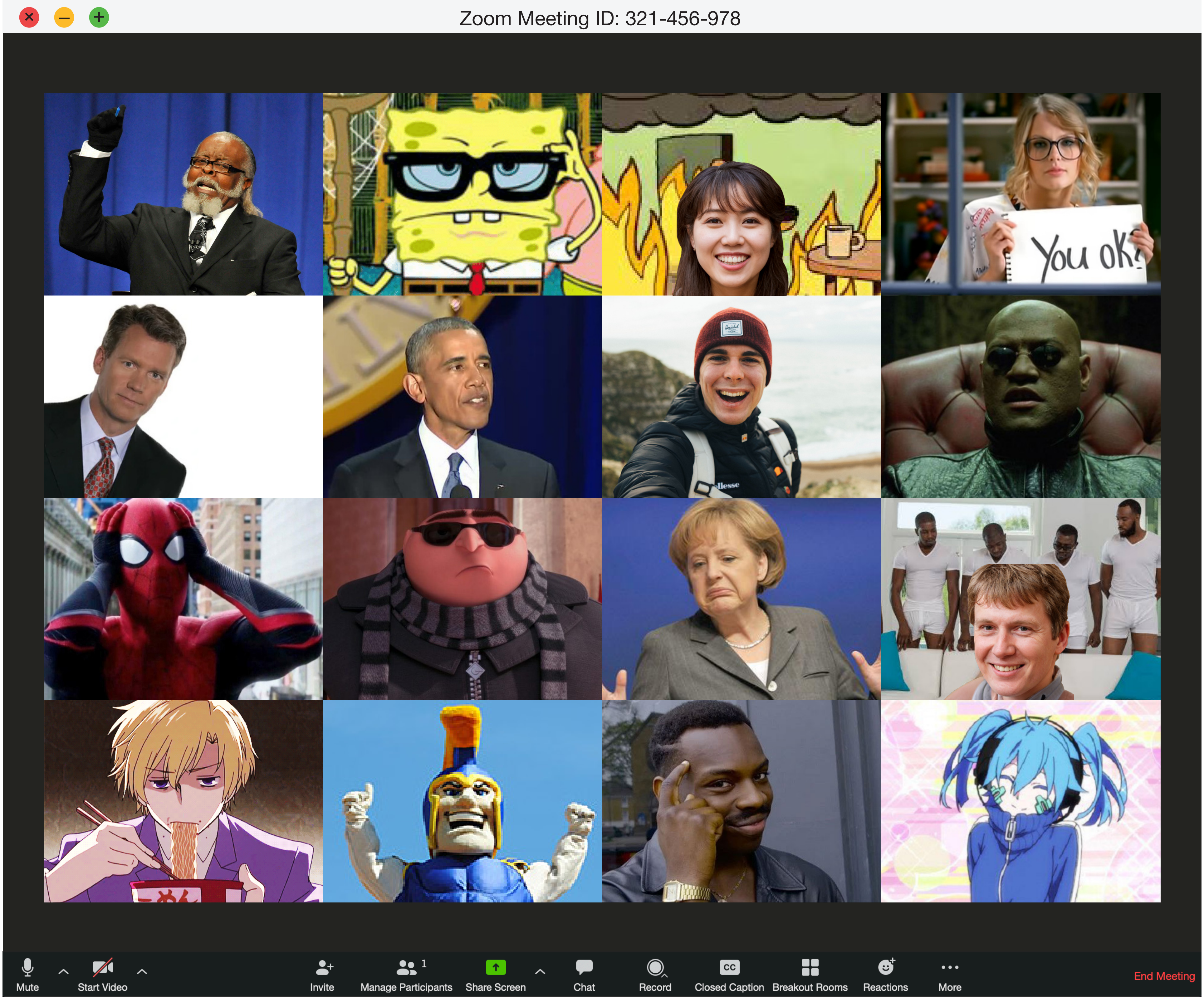

PHOTO ILLUSTRATION BY KUNAL MEHTA AND MARCI SUELA

# Zoom poses risks for students

## Video conferencing software raises concerns about privacy, security

Kunal Mehta
SCIENCE & TECH EDITOR

I really haven't enjoyed sheltering in place for the past three weeks, but one thing has made it slightly more bearable: Zoom memes.

Across the world, college students are signing onto Zoom for the first time as classes are forcibly shifted online because of the coronavirus pandemic and then making jokes about it.

Widely used in the business world, Zoom and other teleconferencing software allow for professors and students to interact in a setting that is probably as close to an in-person classroom as possible.

With the ability to raise your hand, chat with fellow students and make silly faces behind your professor's back, it's a testament to modern computing technology that such a thing is possible in the first place.

But like all technology, Zoom has its downsides.

Zoom has a track record of poor privacy and security management practices that especially affect students who have no option but to use it.

As a newly enrolled student of Zoom University, these are my main fears:

First off, the host of a Zoom call can see any direct messages sent through Zoom's chat. In other words, don't try to slide into your classmate's DMs through Zoom if you don't want your professor to read the messages too.

Zoom hosts can also see whether you've switched over to a different window and no longer have your class front and center. Only the application can see what you're focusing on, so using Zoom in your web browser will protect you – more on that later.

But it gets really creepy when we take a look at what the administrators of our Zoom accounts can see. In this case, that's San Jose State staff members. In a 2015 demo video, a Zoom sales executive showed off the excessive data collection and reporting features of the product.

Zoom administrators can see how much time you spend on Zoom, where you are connecting from (IP address), whether your video was enabled and what type of computer you're using. They can even see the make and model on the audio device you were using, such as the specific kind of headphones you were wearing.

Could you imagine a university administrator coming into your class to write down what kind of headphones each student has? It would be a complete invasion of privacy for no justifiable reason.

Here's the kicker: whoever is assigned as a Zoom administrator at SJSU could join your class meetings with no advance notification. In some of my classes, I would definitely be uncomfortable having normal conversations with my professors if an administrator could barge in with no notice.

Realistically, what options do we have? Our tuition money pays for SJSU's education plan with Zoom and the university seems unlikely to change course given all the other problems it needs to deal with right now.

The main takeaway I have is to use Zoom through your web browser rather than installing its application, as I had mentioned earlier. Your web browser acts as a digital sandbox, preventing Zoom from accessing most of the private information about you on your computer.

The major web browser manufacturers design them to protect users against malicious websites, and in this case Zoom does act maliciously.

Using Zoom in a web browser would have protected users in 2019 when a security researcher disclosed a serious flaw in the Zoom macOS application. Installing the app on your Mac would also install a second piece of software that effectively allowed any malicious website to force users to join a Zoom video call with their webcam enabled, without any prompt or confirmation step.

Despite the obviously problems, Zoom initially doubled down on the functionality, defending it as providing a better user experience because there was no confirmation step when intentionally joining a meeting, according to a July 2019 story on Ars Technica, a technology news website. Apple didn't agree with Zoom and pushed an update to remove the malware from all macOS computers until Zoom reversed its stance and removed the functionality itself.

While most apps have security flaws, it's especially concerning that a company would intentionally introduce them and then try to defend the flaws once it's pointed out how problematic they are.

I should make it clear that I don't blame the SJSU administration nor professors for the current situation we're all in today. Zoom leads the market in comparable software solutions and is probably better than whatever else is available.

But as students, we must stand up for our own privacy rights. Whenever an event triggers a mass crisis, citizens lose rights that never return.

After 9/11, the Patriot Act and similar ensuing legislation gave the government broad spying powers that still infringe upon our civil liberties to this day. It's likely that similar legislation will be passed during the COVID-19 pandemic.

On Saturday, Politico reported that the U.S. Department of Justice wanted to partially suspend habeas corpus rights by allowing judges to indefinitely detain people during the national emergency, opening a slippery slope for every future emergency.

It is just as likely that if this experiment of moving all classes online doesn't end in a total disaster, SJSU will move forward with more online classes, relying even more heavily on technologies such as Zoom.

Although there is no stopping the inevitable increase of classes that use Zoom in the future, it is imperative that students' privacy rights are respected.

Only then can we safely enjoy our memes.

## Tips for students to protect themselves

**1 Only use Zoom through your web browser**

Web browsers will digitally sandbox Zoom, limiting the amount of private information it can access.

**2 Don't send private DMs through Zoom**

Your professor can read all chat messages sent through a Zoom call, even if they are private to a specific user.

**3 Advocate for student privacy rights**

SJSU will likely embrace more online technology in the future, making it important that students stand up for their rights.

**Follow Kunal on Mastodon**
**@legoktm@mastodon.technology**

*Binary Bombshells appears every other week on Thursday.*